

# **Blockchain Technologies: Application and Challenges**

**(Libra cryptocurrency)**

**Written by**

Gan Chun Hooi, Jerry

On

**1st September 2019**

## Introductory overview of Facebook Libra

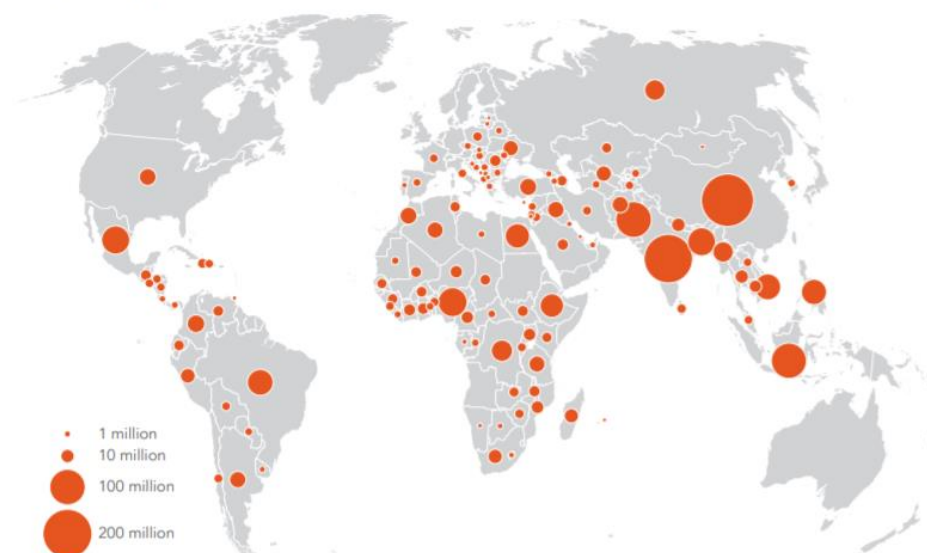
Libra, the cryptocurrency by Facebook has garnered much public attention after the announcement in June 2019 and it target to launch in first half of 2020. Libra has become a hot topic among folks for their big idea of blockchain and there are much discussion is Libra in fact a true cryptocurrency, but definitely there is no doubt that this is a significant event for the blockchain industry. (Teo, 2019) Libra is planning for a new decentralized blockchain, a stablecoin with low volatility and smart contract platform together that leap forward towards a lower cost, more accessible and global connected financial system. The mission of Libra is to create a simple global currency and financial infrastructure that can empowers billions of people. (Association, 2019).

Facebook named their cryptocurrency as 'Libra' meaning free from French word 'libre'. it consist unit of measure from ancient Roman, the astrological symbol depict the scales of justice and resemblance the French libre, to form "A combination of money, justice and freedom". (Barber, 2019)

## What Libra intends to solve and do

Libra's vision is to create a new decentralized blockchain with a stable global cryptocurrency to serve the underserved. Based on current world population, there are still globally about 1.7 billion adults remain outside the financial system without a bank account and there are major unbanked in developing countries in ASEAN situated in countries such as Myanmar, Cambodia, Laos, Indonesia, Philippines and Vietnam. (Asli Demirgüç-Kunt, 2018)

**Globally, 1.7 billion adults lack an account**  
Adults without an account, 2017



Source: Global Findex database.

Note: Data are not displayed for economies where the share of adults without an account is 5 percent or less.

People around the world pay high fees, from remittance to wire cost, ATM charges and pay loans can charge interest rates up to 400 percent. For those who remain "unbanked", the fees are too high and banks is too far way and they are lack of documentation. (Association, An Introduction to Libra, 2019)

The current blockchain system still yet to achieve mainstream adoption. Therefore, Libra the cryptocurrency by Facebook, is designed for payments services range from micropayments to

remittance services with nearly zero fees, so it is as easy as sending money like email to lower down the cost, to be more accessible and achieve financial inclusion.

Libra just like cash inside the phone. User able to buy or cash out Libra online at local exchanges or potentially pay for things like Uber or Spotify for those companies that partnered with Facebook in Libra to make it popular. Libra will be as easy to spend like message through Facebook wallet apps, Calibra which will be available on WhatsApp, Messenger and through a standalone app.

In order to ensure the data and privacy protection, Facebook set up Calibra, a new subsidiary regulated digital wallet platform to ensure separation between social and financial data and build operating services on top of Libra network. (Constine, 2019)

### Existing solutions addressing the same issue

Facebook Libra is trying to build a payment system that combine the best characteristics of blockchain and conventional networks. Libra act like similar to Bitcoin and it changes some of the important ways to avoid bitcoin networks shortcomings.

The main difference between Libra and Bitcoin is that the bitcoin network is fully open to all, but not for Libra. In bitcoin, anyone with can participate in mining process to verify bitcoin transactions. By contrast, the participation in the Libra's transaction clearing process is only limited to the founding members. (Lee, 2019)

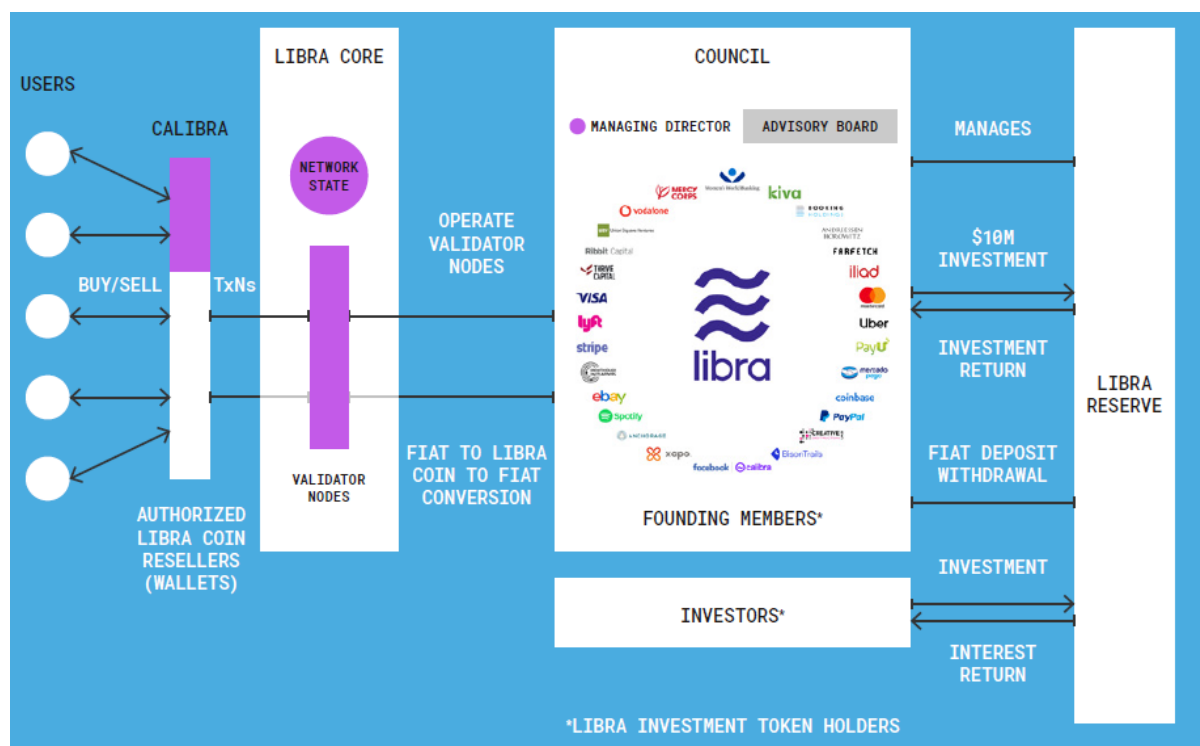
Based on Libra's technical whitepaper, Libra's protocol able to support 1,000 payment transaction per second (TPS), while bitcoin can only perform 7 Transaction per second (TPS). This is because Libra network is only managed group of validated nodes called 'Founding Members', therefore it is not truly decentralised. Bitcoin network added new block to the blockchain on average about 10 minutes, while Libra aim for a shorter 10 seconds finality time. (Lee, 2019)

Aside from that, China's central bank also will launch a state-backed cryptocurrency and it will issue to seven big institutions such as Alibaba and Tencent in coming months to disperse the cryptocurrency to 1.3 billion Chinese citizens and other businesses doing in the renminbi, China's fiat currency. China DC/EP (Digital Currency/Electronic Payments), the technology behind the cryptocurrency could target to launch on November 11, which known as Singles Day of China's busiest shopping day. Recently, Bank of England governor Mark Carney also floated the idea of new currency backed by a number of central banks to replace US dollar. (Castillo, 2019)

## Rationale and the design of token economy

The Libra coin is backed by reserve asset that pegged to a basket of stable international currencies to create stability value of Libra. Libra is a “stablecoin”, a stable currency that backed by a reserve of real assets unlike conventional cryptocurrency where the price is very volatile. Libras will be fully reserved. Basically every time when a user transfer money to get Libra, new money are created and the money will go into the Libra reserve pegged pools of reserved currencies, and it will stay there until the customer withdraws the money from the system. (Barber, 2019)

The design economy of the Libra token ecosystem can be simplify as outlined in diagram below (Brennan, 2019);



## Libra Network and Libra Association

Libra will start as a ‘permissioned’ blockchain, meaning it is not truly decentralised and not anyone can set up a node to join the network. For security and regulatory reasons, Libra network will be managed by ‘Founding Members’, a group of validated nodes, where currently there are 28 companies including some big companies in the world like Paypal, Visa, Mastercard, big tech company like Facebook, Uber and Spotify, cryptocurrency services companies like Coinbase and venture capital companies such as Union Square Ventures. All members in Libra association will have equal votes and only the members of the association can run the nodes and validate Libra’s transactions. The association hope to increase to approximately 100 members at the initial launch date. (Association, 2019).

The criteria’s of becoming a member of the Libra association are exclusive. Their business need to have market value greater than \$1 billion dollar, business reach at least 20 million a year and it need

to be among the top 100 from fortune 500 companies or top 100 from Charities or academic institutions.

Refer figure below the current founding members as of August 2019 with the association governed by diverse businesses, non-profit and multilateral organizations, and academic institutions.



Over time, the Libra association will develop towards permissionless and move toward increasing decentralization.

The **interest earn** from the reserve assets will only go to founding members after deduct the cost of operation and investment in technology for development of Libra. Founding members earn a cut of the interest in proportion to how much they invested when they joined. Therefore, user of Libra will not receive any return from the reserve. The distribution of interest earn from Libra seems not "Benevolent" as it only benefits to the founding members and it is not share among all or to the whole community. If the reserve grows huge and many people use it, the interest could be end up good revenue for Facebook only, but not for the community. This reward system seems only benefits to Facebook and its founding members. In order to achieve "Benevolent" (to share), it should empower everyone so that it can achieve sustainable grow for the community.

## Design thinking behind Libra blockchain application

The design thinking behind Libra blockchain for the development of Libra consensus is based on Libra BFT and it use new programming language called "Move".

### Using Move Programming Language

Move is a new programming language created by Facebook that based on Rust. The key feature of Move is the ability to define custom resource types with linear logic, so that the resource can never be copied or implicitly discarded. It only moved between program storage locations. (Sam Blackshear, 2019) It's called Move because its primary function is to move Libra coins from one account to another and never let those assets be accidentally duplicated.

### Libra BFT consensus protocol and State Machine Replication

Libra adopted Byzantine Fault Tolerant approaches in their consensus protocol to facilitate agreement among all validator nodes (refer to founding members) on the transactions to be executed and the order they are executed. (Association, 2019). In Byzantine fault-tolerant system, we assume nodes can fail or to be malicious. Therefore, BFT are designed to function correctly even some of the validator nodes, up to one third of the network which is 33% are compromised or fail. Libra BFT system enables high transaction output and low latency environment.

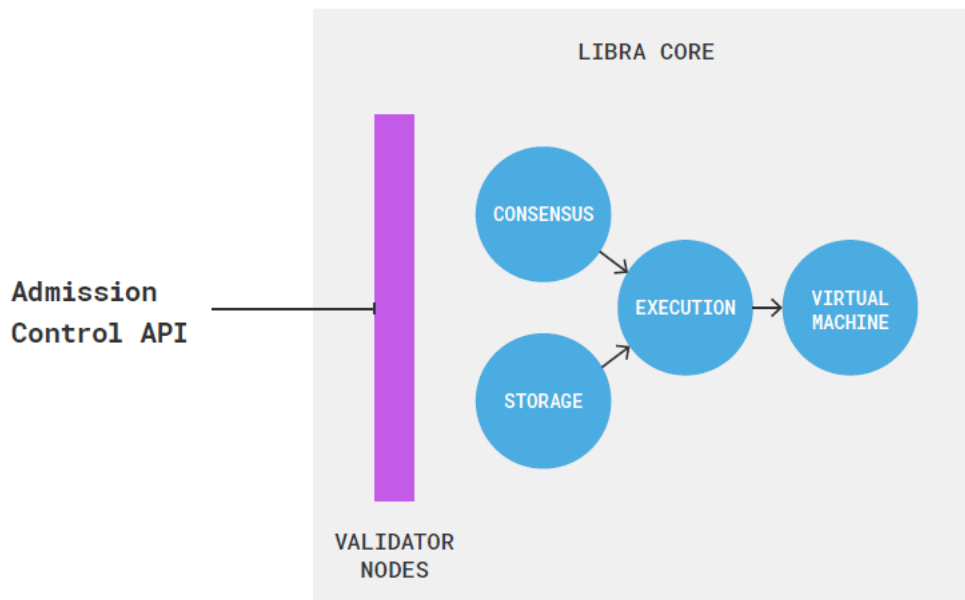
LibraBFT consist the following key properties; (Association, State Machine Replication in the Libra, 2019)

1. Safety (something bad will happen) - LibraBFT maintains consistency among honest validators, even if up to one-third of the validators are corrupt.
2. Asynchronous (aka toki toki) – Asynchronous transmission, also called as start/stop transmission is simple, fast and cost effective as compare with synchronous transmission. Consistency is guaranteed even in cases of network asynchrony i.e. during periods of unbounded communication delays or network disruptions.
3. Finality- LibraBFT supports a notion of finality, whereby a transaction becomes irreversibly committed.
4. Linearity and Responsiveness
5. Simplicity and Modularity - allows simple and robust implementation, in line with public blockchains based on Nakamoto consensus.
6. Sustainability - LibraBFT is designed as a proof-of-stake system, where reward to good behaviors and punish wrongdoings from stakeholders. Computational costs of LibraBFT consist primarily of cryptographic signatures, not like POW consume vast amounts of energy and computational power.

The design thinking behind Libra cryptocurrency uses Libra BFT and State Machine Replication protocol for implementing fault-tolerant service by replicating servers and coordinating client interaction with server replicas to guarantee liveness and safety. The state machine distributed over the network and the whole network run as interconnection of copies, called nodes.

## Distribution of Trust in Libra

Libra BFT is a leader-led consensus model by vote, meaning the founding members will take turn authorizing the transactions that are coming into the network. The diagram below shows the Libra validator execution.



In the Libra validator execution, all the calls to the network go through a single API, called Admission Control. There is strict control on the network traffic which means the demand on the validators will be high. This is a more centralized model unlike Ethereum and Bitcoin where anyone can submit a transaction or run a node. This is the trade-off for Libra in order to achieve speed and security. For instance, Calibra, the authorized Libra coin reseller (wallet) by Facebook's own app, will be acting as intermediaries just like Coinbase. Users will need to go through this centralized server to interact with the Libra network. Therefore, there is NO distribution of trust in the design of Libra as it has only limited numbers of actors and it depends on a centralized server.

## Privacy Protection

One of the most important key elements cannot be missed in the design of a token is privacy protection. The word 'Privacy' is only mentioned once in the Libra whitepaper. Libra's ambitions to empower billions of people and the Libra network will be handling huge amounts of user data and Libra is starting with a 'permissioned' blockchain, with founding members as the validator nodes. This creates a great opportunity for Libra to understand customer behavior and privacy data beyond their current scope. Therefore, data privacy should be seriously considered and well planned through in the design in order to avoid serious data leaks and misuse of data to be happened. In an open data platform, owners of data will have control over their own data while keeping it private and safe. This is the way forward to enable data-driven technology in a highly regulated world. (Teo, 2019)

## Appraise the overall design of Libra blockchain application

Libra is adhered to LASIC principles, where It is low-margin, asset-light, scalable, innovative and compliance-easy. But the privacy protection and data concerns shall be well planned through in the design in order to avoid serious data leaks and misuse of data to be happened.

For Libra, every additional fiat currency in the reserve will be a regulatory challenge. Libra may have the vision to become an independent decentralised blockchain to serve the underserved. However, the weakest point will be its links to fiat currency that makes it seem to be stabled. (Teo, 2019) For example in United States, if want to register as money transmitters where they operate, and many states require money transmitters to post bonds to ensure they won't defraud customers. And this is just in United States. Other governments around the world have their own rules. There is "serious concern" for regulator as highlighted by Federal Reserve Chairman, Jerome Powell signalled scepticism about Facebook's Libra cryptocurrency plan. Powell said in testimony that he don't think the project can go forward without broad satisfaction with the way the company has addressed money laundering. (Lee, 2019)

There is another thing you may noticed in the Libra Association. There are no big banks signed on at launch and big tech giant in the Libra partners like Google, Apple and Amazon in the list. One may also find why Libra set up headquartered in Geneva, Switzerland but not in United States.

Libra complied to 3C's (**Community, Creativity, Compassion**). For 5D's, Libra can only meet the first 3Ds which is **Digitalisation, Disintermediation** and **Democratisation**, which tech giant like Alibaba able to meet the first 3Ds. But for the 4D's "**Decentralisation**" which is crucial for crossing border. Libra technology is decentralised, but with centralised governance. It is not truly decentralised as not anyone can set up a node to join the network and it is only limited to the founding members which only seems to further centralize power. For the last, which is the 5D's "**Diminishing**" oneself like stated in Satoshi's whitepaper. Libra seems unable to meet the last 'D' where diminishing will create social scalability. The facilitator must disappear and diminish so that the project can scale and cross border.

Libra can achieve technical scalability, but not social scalability. Social scalability is the ability to overcome the mind-set that limits who or how many can successfully participate. Social scalability is about human limitation, not about technical limitations. Only an open network has high social scalability. In Inclusive blockchain, it will have both technical scalability and social scalability.

The Libra team hiring is led by David Marcus, ex-PayPal president and he is one of the early Bitcoin investor who also serves on the Coinbase board. The recruitment team of Libra consist company's top engineers, top economists and policymakers. The team has grown to more than 50 employees including the former team behind blockchain startup, Chainspace. The team diversity seems majority are main from US big tech companies and not diversify in nationality as it is not clearly stated in the white paper. The competency of Libra team is strong and some of the members have track record in blockchain project experience.

Therefore, in summary for a blockchain project to be successful and sustainable, the project shall adhere to all the essential features of 3C's, 5D's, LASIC, Open source, Benevolent (to share) and Global (to reach).



## References:

<https://libra.org/en-US/white-paper/>

[https://globalindex.worldbank.org/sites/globalindex/files/2018-04/2017%20Index%20full%20report\\_0.pdf](https://globalindex.worldbank.org/sites/globalindex/files/2018-04/2017%20Index%20full%20report_0.pdf)

<https://developers.libra.org/docs/assets/papers/libra-consensus-state-machine-replication-in-the-libra-blockchain.pdf>

<https://www.entrepreneur.com/article/336776>

<https://pages.consensys.net/understanding-libra>

<https://arstechnica.com/tech-policy/2019/07/facebooks-half-baked-cryptocurrency-libra-explained/>

<https://www.wired.com/story/ambitious-plan-behind-facebooks-cryptocurrency-libra/amp>

<https://www.forbes.com/sites/michaeldelcastillo/2019/08/27/alibaba-tencent-five-others-to-recieve-first-chinese-government-cryptocurrency/#1ae82e51a516>

<https://libra.org/en-US/permissionless-blockchain/#overview>

<https://developers.libra.org/docs/assets/papers/libra-move-a-language-with-programmable-resources.pdf>

<https://techcrunch.com/2019/06/18/facebook-libra/>